REMARKS

Applicants have carefully reviewed the arguments presented in the Office Action and respectfully request reconsideration of the claims in view of the remarks presented below.

Claims 25, 29, 41-42 and 47 have been cancelled and claims 1, 8, 10, 13, 14, 19, 21, 23, 24, 27, 33, 38, 43 and 46 have been amended. Thus, claims 1-24, 26-28, 30-40 and 43-46 are pending in the application.

Claims 13-14, 19, 21 and 23 were objected for various informalities. These claims were amended as appropriate to address the informalities noted by the Examiner, and also to correct inadvertent typographical errors. No new matter was added.

Claims 24 and 26 were rejected under 35 U.S.C. 102(b) as being anticipated by Tomkow (WO 01/10090). Applicant traverses these rejections. It is axiomatic that for a claim to be anticipated, each and every element of the claim must be found within the cited art. The various elements recited in claim 24, contrary to the Examiner's position, are neither disclosed nor suggested by the description and drawings of Tomkow.

Claim 24 recites receiving a message and a compressed encrypted version of the message from a recipient at a web site providing at the server for an indication of the authenticity of the message. Claim 24 then recites decompressing the message to provide a first digital fingerprint of the message, and then decrypting the compressed encrypted version of the message to provide a second digital fingerprint of the message. In contrast, Tomkow does not disclose the step of providing at the server a compressed encrypted version of the received message; Tomkow only discloses, on pages 41 and 42, detaching and decrypting a digital signature that has been attached to the message, hashing the remainder of the document, and then comparing the two hashes. Moreover, Tomkow does not teach or even suggest the step of decompressing the message to obtain a first digital fingerprint and then decrypting the compressed encrypted version of the message provided at the server to provide a second digital fingerprint for comparison. According, Applicant respectfully submits that claim 24, and the claims dependent therefrom, are neither anticipated by, nor rendered obvious by the teachings of Tomkow. The Applicant therefore requests that the rejection be withdrawn and that claim 24 and its dependent claims be allowed.

Claims 1-23, 27-28, 30-32 and 40 were rejected under 35 U.S.C. 103(a) as being unpatentable over Tomkow, and further in view of Meyer et al. (US 2002/0143871). Applicant traverses these rejections.

Claim 1 has been amended to recite the steps of generating at the server a digital signature of the message, attaching the digital signature of the message to an HTML file at the server, the HTML file also including the identity of the sender in plain text, and attaching the html file to the message at the server, transmitting from the server to the recipient the message and the attachment, receiving the message and the attachment at the server from the recipient, providing digital signatures of the message and the attachment at the server, and authenticating to the recipient the message and the attachment at the server on the basis of the information received by the recipient form the server and on the basis of the digital signatures provided by the server. As admitted by the Examiner, nowhere does Tomkow teach or even suggest attaching an HTML file including a digital signature of the message to the message.

However, Applicant respectfully submits that the Examiner's reliance on Meyer to provide the missing step is misplaced. Meyer does not teach or even suggest, nor would one skilled in the art readily understand from reading Meyer, the steps of generating a digital signature of the message at the server, attaching the digital signature to an attachment that is not part of the message to the message, and then authenticating the message to the recipient, as is claimed in amended claim 1. Meyer only discloses converting plain email text to HTML (See, ¶¶ 90, 135). Meyer embeds meta content in the email as an object (See, ¶¶ 8, 14, 43 and 142). Moreover, Meyer discloses embedding such content in "index fields" into the converted document, not including an embedded string in a separate HTML document that is then attached as a separate document to the original email, as is claimed in amended claim 1. Given the Examiner's statement that Tomkow also does not disclose the attachment of a separate HTML file to a message, combining Tomkow and Meyer still would not provide to one skilled in the art the novel combination of steps contained in amended claim 1. For these reasons, Applicant respectfully submits that amended claim 1 and its dependent claims are patentable over the cited art and request that the rejections be withdrawn and that claim 1 and its dependent claims be allowed.

Similarly, claims 8 and 14 were also amended to recite generation at the server a digital signature of the message, and then attaching or providing an attachment in the form of an HTML file including the digital signature of the message. For all the reasons set forth above with respect to amended claim 1, Applicant believes that amended claims 8 and 14, and also their respective dependent claims, are patentable over the cited art. Accordingly, Applicant requests that the rejections be withdrawn and that claims 8 and 14 and their respective dependent claims be allowed.

Claim 27 was amended the recited that the attachment separate from the message that is received at the server is in the form of an HTML file and contains information about delivery of the message to the recipient and a digital signature of the message. Again with reference to the arguments set forth above with respect to amended claim 1, neither Tomkow or Meyer, alone or in combination teach or even suggest providing a separate HTML file attached to a message, the contents of which are then used to determine the authenticity of the message, as is claimed by amended claim 27. For these reasons, Applicant respectfully requests that the rejection of claim 27 as amended be withdrawn and that claim 27 and all of its dependent claims be allowed.

Similarly, claim 40 is also believed to be patentable over the combination of Tomkow and Meyer because neither of those references, taken alone, or in combination, teach or even suggest digitally sealing the encrypted has of the a hashed string by attaching the encrypted hash of the hashed string to an HTML file and sending to the recipient a message and the HTML file including the encrypted hash of the hashed string, as is claimed in claim 40. As stated previously, the Examiner stated that Tomkow does not disclose such an HTML file. Moreover, Meyer only discloses converting plain email text into HTML and embedding indexes in the same email. Meyer does not teach attaching an HTML file including an encrypted hash of a hashed string to the message. Accordingly, Applicant submits that claim 40 is patentable over the art of record and requests that the rejection be withdrawn and that claim 40 be allowed.

Claims 43-47 were rejected under 35 U.S.C. 103(a) as being unpatentable over Tomkow and Meyer, and further in view of Stark et al (US 2002/0131566). Applicant respectfully traverses these rejections.

Claim 43 as amended recites providing at the recipient a compressed and encrypted string including an identification of the sender, the message, a hash of the attachment and an embedded

has of the string, decompressing the string, decrypting the decompressed string, hashing the string less the embedded hash of the string, and then comparing the hash of the string less the embedded hash of the string and the embedded hash. Contrary to the Examiner's position, Tomkow does not disclose these steps. Tomkow discloses, on pages 41 and 42, only that "the system generates a hash of the balance of the document, and one for each file attached to the message. In steps 1003 and 1004, the hashes are compared." This is not the same as providing a string that contains information plus an embedded hash of the string, wherein decompressing the string and decrypting the decompressed string provide a decompressed, decrypted string that is then hashed, leaving out the embedded hash of the string. The hash of the string less the embedded hash is then compared with the embedded hash. These are additional steps that are not disclosed by Tomkow, Meyer or Stark.

Further, while Stark does disclose the concept of compressing information to make an email smaller, Stark does not teach or even suggest providing a compressed and encrypted string including an identification of the sender, the message, a hash of the attachment and an embedded hash of the string, decompressing the string, decrypting the decompressed string, hashing the string less the embedded has of the string, and comparing the hash of the string less the embedded hash of the string and the embedded hash, as is claimed in amended claim 43. Even combining the teachings of Stark with Tomkow, it would not have been obvious to one skilled in the art at the time of the invention to carry out all the steps claimed in amended claim 43 because those steps are not taught or even suggested by the combined references. Not even if the references are combined using impermissible hindsight is amended claim 43 taught or suggested by those references.

Moreover, the Examiner's rejection states that claim 43 is unpatentable of Tomkow and Meyer, further in view of Stark. Meyer is not even a proper reference against claim 43 because Meyer teaches nothing that is recited by the claim, and indeed, is not mentioned anywhere in the specific description of the rejection.

For all of these reasons, Applicant respectfully submits that amended claim 43, and the claims dependent thereon, are patentable over the cited art, and requests that the rejections be withdrawn and that claims 43 and its dependent claims be allowed.

Claim 46 was rejected similarly to claim 43, for the same reasons. Accordingly, the arguments directed to amended claim 43 apply equally well here. Amended claim 46 recites the steps of providing at the recipient an encryptment of a string including information relating to the identification of the sender, the attachment and the message stripped of the attachment and a hash of the string. Nowhere does Tomkow, on pages 41 and 42, or anywhere else in the reference, teach or even suggest such a limitation. Tomkow discloses, on pages 41 and 42, only that "the system generates a hash of the balance of the document, and one for each file attached to the message. In steps 1003 and 1004, the hashes are compared." This is not the same as providing a string that contains information relating the identification of a sender, an attachment and a message stripped of the attachment plus a hash of the string, wherein the information relating to the identification of the sender, the attachment and the message stripped of the attachment is hashed, leaving out the hash of the string. Further, Tomkow does not teach or suggest comparing the hash of the string separated from the string and the hash formed from the information in the string (without the hash of the string) to authenticate the receipt, as is claimed in amended claim 46.

Again, even though Stark does disclose the concept of compressing information to make an email smaller, Stark does not add anything further to Tomkow to provide one skilled in the art with the combination of steps recited in amended claim 46. For example, even combined, Tomkow and Stark do not teach or even suggest providing an encrypted string including information relating to the identification of the sender, an attachment, the message stripped of the attachment and hash of the string, decrypting the string, separating the hash of the string from the string, forming a hash from the information relating to the identification of the sender, the attachment and the message striped of the attachment, and comparing the hash of the string separated from the string and the hash formed from the information in the string, as is claimed in amended claim 46. Not even if the references are combined using impermissible hindsight is amended claim 46 taught or suggested by those references.

For all of these reasons, Applicant respectfully submits that amended claim 46 is patentable over the cited art, and requests that the rejections be withdrawn and that claim 46 be allowed.

Claims 33-37 were rejected under 35 U.S.C. 103(a) as being unpatentable over Tomkow and Meyer, and further in view of and Stark. Applicant traverses these rejections.

Claim 33 was amended to recite that the attachment is in the form of an HTML file that is not part of the message, with attachment including a digital signature of the message. In other words, the attachment is not part of the original subject matter of the message, which may have included documents or files known to many as "attachments" which are different from the attachment claimed, and will be clear to one skilled in the art from numerous examples discussed in the specification of the application as filed. Tomkow only discloses appending an encrypted digital signature or digital digests to a message. Tomkow does not teach or even suggest sending an attachment that is not part of the message to a server where the attachment is then used to assist in authenticating the message, as is claimed in amended claim 33. Moreover, contrary to the Examiner's position, Tomkow does not disclose or even suggest providing at a server and compressed encrypted version of the combination of the message and the attachment and decompressing the combination in accordance with a particular compression to provide first digital fingerprint of the combination, and then decrypting the compressed encrypted version of the combination of the message and the attachment in accordance with the particular encryption to provide a second digital fingerprint of the combination and then comparing the first and second digital fingerprints of the combination of the message and the attachment to determine the authenticity of the message and the attachments, as is claimed in amended claim 33. Applicant has reviewed the portion of the Tomkow reference cited by the Examiner for support of the rejection but finds no disclosure at all pertaining to comparing first and second sets of digital fingerprints to determine authenticity of the message and the attachment.

Further, as discussed above with reference to amended claim 1, among others, Meyer does not teach or even suggest, nor would one skilled in the art readily understand from reading Meyer, the steps of generating a digital signature of the message at the server, attaching the digital signature to an attachment that is not part of the message to the message, and then authenticating the message to the recipient, as is claimed in amended claim 1. Meyer only discloses converting plain email text to HTML (See, ¶¶ 90, 135). Meyer embeds meta content in the email as an object (See, ¶¶ 8, 14, 43 and 142). Moreover, Meyer discloses embedding such content in "index fields" into the converted document, not including an embedded string in a separate HTML document that is then attached as a separate document to the original email, as is

claimed in amended claim 33. Given the Examiner's statement that Tomkow also does not disclose the attachment of a separate HTML file to a message (with reference to claim 1), combining Tomkow and Meyer still would not provide to one skilled in the art the novel combination of steps contained in amended claim 33.

Moreover, the Examiner cites Stark et al. as teaching compression of the combination. However, even taking the combination of art as suggested by the Examiner, for the reasons stated above, one skilled in the art and being aware of both Tomkow and Stark et al would still not obtain the novel method claimed in amended claim 33. For these reasons Applicant submits that claim 33 is not obvious in view of the cited art, taken alone or in combination as suggested by the Examiner, and respectfully requests that the rejection be withdrawn and that claim 33 and the claims dependent therefrom be allowed.

Claims 38-39 were rejected under 35 U.S.C. 103(a) as being obvious in view of Tomkow and Kaufman et al (US Patent No. 5,764,772). Applicant traverses this rejection. Claim 38 has been amended to correct an inadvertent typographical error.

The Examiner states that Tomkow on page 40 teaches "digitally sealing the encrypted hashed string by attaching the encrypted hashed string to an HTML file and attach the HTML file including the encrypted hashed string to the message." However, this is inconsistent with the Examiner's statement in his rejection of claim 1 that "Tomkow failed to disclose that the attachment was an HTML file. . . ." Further, nowhere can the words "digitally sealing" be found within Tomkow. Digitally sealing, as that phrase is defined by the pending application, is only disclosed in the pending application, and is nowhere defined, illustrated or discussed within Tomkow.

Moreover, as discussed above, not only does Tomkow fail to disclose attaching an encrypted hash of the hashed string to an HTML file (as admitted by the Examiner on page 17, lines 8-9 of the Office Action), but Meyer is no help here either, for all of the reasons stated previously.

There is simply no disclosure or even a suggestion of the "digital sealing" method claimed in amended claim 38 to be found in any of the cited art. While Tomkow does disclose attaching a digital signature to a message, there is no teaching that such a simple digital signature can be considered the same as the method of digital sealing which includes attaching an HTML

file to a message as claimed by Applicant. Moreover, adding Kaufman to the mix still does not provide to one skilled the art the invention claimed in amended claim 38, because Kaufman fails to teach or even suggest attaching even a multiply hashed string to an HTML file and attaching the HTML file including the hashed string to a message. Applicant submits that claim 38, and claim 39 dependent therefrom, is patentable over the cited art. Accordingly, Applicant respectfully requests that the rejection be withdrawn and that claim 38, and claim 39 dependent therefrom, be allowed.

CONCLUSION

Applicants have carefully reviewed the arguments presented in the Office Action and respectfully request entry of the amendment and reconsideration of the claims in view of the remarks presented. In light of the above amendments and remarks, Applicants respectfully request that a timely Notice of Allowance be issued in this case.

Should the Examiner have any questions concerning the above amendments and arguments, or any suggestions for further amending the claims to obtain allowance, Applicants request that the Examiner contact Applicants' attorney, John Fitzgerald, at 310-242-2667.

The Commissioner is authorized to credit any overpayment or charge any additional fees in this matter to our Deposit Account No. 06-2425.

Date: July 1, 2008

Respectfully submitted,

FULWIDER PATTON LLP

By: /john k. fitzgerald/
John K. Fitzgerald
Registration No. 38,881

JKF:vmm
Howard Hughes Center
6060 Center Drive, Tenth Floor
Los Angeles, CA 90045
Telephone: (310) 824-5555
Facsimile: (310) 824-9696
Customer No. 24201
226789.1